UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

STEVEN FLOYD, on behalf of himself and all others similarly situated,

Plaintiff,

v.

AMAZON.COM, INC., a Delaware corporation, and APPLE INC., a California corporation,

Defendants.

Case No. 2:22-cv-01599-JCC

JOINT STATEMENT OF DISPUTES REGARDING PROTECTIVE ORDER AND ESI PROTOCOLS

Pursuant to the Court's scheduling Order (ECF No. 48), the Parties have worked in good faith to reach agreement on (1) a Protective Order and (2) an Order Regarding Expert Discovery ("Expert Discovery Protocols"). While the Parties have made substantial progress on these documents, they were not able to resolve all disputes. The disputed issues that remain, and the Parties' respective positions on each, are set forth below.

1. Protective Order

Plaintiff's Statement:

The Parties have reached agreement on most aspects of the Protective Order, but disputes remain on provisions relating to (1) data security and (2) disclosures outside the U.S. and to foreign nationals. On both issues, Defendants propose procedures and restrictions that would depart dramatically from this District's Model Stipulated Protective Order. The departures are not justified, as set forth below. Plaintiff respectfully requests that the Court enter the Protective Order Plaintiff has proposed, attached hereto as Ex. A.

Data Security. Defendants propose an elaborate and unworkable set of "data security" provisions that go far beyond this District's Model Stipulated Protective Order. Under these proposed provisions, Parties would need to certify compliance with certain detailed information security management system ("ISMS") protocols. *See* Ex. B at § 9(1). Thereafter, Parties could only access designated materials using "multi-factor authentication" and would need to "implement encryption" to transmit designated material outside their "network(s)" (a term that is not defined). *See id.* In the event of a "Data Breach" (defined broadly to include any potential unauthorized disclosure of designated material or "devices" containing it), Parties must disclose to their litigation adversary the details of their data security systems, including "vulnerabilities or flaws," submit to formal discovery as to the breach, negotiate potential extensions to the case schedule, and follow other elaborate procedures. *See id.* § 9.

Defendant Apple recently sought to impose similar requirements in *Societe Du Figaro, SAS, et al., v. Apple Inc.*, 22-cv-04437 (N.D. Cal.) ("*Figaro*"). The *Figaro* court rejected them in full. *See* Ex. E at 2-6. Plaintiff respectfully submits this Court should do the same. This is not

because data security is unimportant. It is because Defendants' proposal is unnecessary and unworkable.

First, this Court's Model Order already addresses data security and the "model order is the model for a reason—it was drafted and approved by judges of this district based on their collective experience managing numerous cases with confidential material." *Kater v. Churchill Downs Inc*., 2020 WL 13490764, at *2 (W.D. Wash. May 5, 2020); *see also Taladay v. Metro. Grp. Prop. & Cas. Ins. Co*., 2015 WL 4494561, at *2 (W.D. Wash. July 23, 2015) (observing that local rules "already set forth an orderly process for protecting confidential information").

Specifically, in provisions Plaintiff adopts in full, the Model Order already requires that parties maintain Protected Material "at a location and in a secure manner that ensures that access is limited to the persons authorized under this agreement." *See* Ex. A § 5.1. Defendants have identified no reason to believe Plaintiff will fail to abide by these security requirements. *See Figaro,* Ex. E at 3 (rejecting requirement that parties certify compliance with detailed data-security standards because "the more general requirement of a secured system is good enough").

Plaintiff has also agreed to enhanced reporting and disclosure requirements (beyond the Model Order) in the event of any unauthorized disclosure. *See id.* § 10. Under Plaintiffs' proposal, if there is an unauthorized disclosure, the Receiving Party must (a) notify the producing party in writing, (b) investigate the "scope of and circumstances of" of the disclosure, (c) "take immediate and reasonable steps to rectify the unauthorized access or disclosure," (d) comply with all appliable security breach notification laws (along with other steps). *See* § 10. These robust protections will facilitate a productive and forceful response to any data breach.

Second, as the *Figaro* court concluded, Defendants' elaborate data security provisions are not workable in practice. *See* Ex. E. The problems are many. For one, it is unclear how Parties could implement multi-factor authentication for "any access" to designated material, including routine emails between counsel. Nor is it clear when a communication extends beyond a party's "network" thus triggering Defendants' encryption requirements, or how encryption could work in the flow of a litigation where Parties must regularly communicate with consultants, court

reporters, document vendors and others authorized to review Protected Material. *See* Ex. B § 9(1). Read literally, Defendants' data security provisions would even seem to bar filing Protected Material with the Court, including under seal, since a court filing presumably would transcend a party's "network" and the ECF system does not support encryption (to Plaintiff's knowledge). While surely this was not Defendants' intent, these types of unintended consequences are precisely why their elaborate data-security provisions should be rejected.

Similar practical problems pervade the measures Defendants propose for "data breaches." To begin with, while Defendants appear to be concerned with cyberattacks or other infiltrations, they define "data breach" to include *any* unauthorized disclosure, as well as *any* "unauthorized access" to "devices." *See id.* § 9(2). Accordingly, the heavy-handed procedures Defendants propose would be triggered if, for example, a court reporter inadvertently neglected to sign Exhibit A before transcribing a portion a deposition, or if a legal assistant accessed a lawyer's "device" without express permission (even without reviewing any Protected Material). This makes little sense, as the *Figaro* court observed. *See* Ex. E at 3-4 (rejecting data breach provisions as "really heavy-handed medicine that would apply to just technical violations of the protective order"). Nor does it make sense for Parties to disclose the "vulnerabilities" of their data security systems to an adversary in litigation, as Defendants here propose. *See* Ex. B § 9(3). If anything, this might "undermine . . . security," as the *Figaro* court again noted. *See* Ex. E at 4.

There are also sweeping ramifications to Defendants' data-breach provisions that reflect a lack of consideration. For example, in the event of a "data breach" (again broadly defined), the receiving party must provide "sworn assurance that Discovery Materials will be handled in the future only by entities not impacted by the Data Breach." Ex. B at § 9(4). Accordingly, if Plaintiff's counsel experience *any* unauthorized disclosure of Protected Material, even a technical violation or a systems breach through no fault of their own, Plaintiff's counsel can no longer "handle" Protected Material. As a practical matter, this would remove Plaintiff's counsel from the case. And this could occur even in circumstances where no Protected Material is

disclosed, *e.g.*, if a "device" belonging to counsel is accessed without authorization, but no Protected Material is reviewed by the party gaining unauthorized access.[1]

For all these reasons, Plaintiff respectfully requests that the Court adhere to the Model Order (as modified by Plaintiff's proposal). The Model Order reflects the considered judgment of Judges in this District as to how data security can be maintained in the context of a litigation, and it works in practice.

Disclosure Outside the U.S. and to Foreign Nationals. Defendants' proposed Protective Order would depart from the this District's Model Stipulated Protective Order by prohibiting parties (as well as their counsel and consultants) from reviewing "Protected Material" (*i.e.*, Confidential or Highly Confidential – Attorneys' Eyes Only) outside the territorial United States. *See* Ex. B at §§ 5.2(b), 5.4(b), 5.7. It would further bar any foreign national from viewing Protected Material within the United States. *See id.* § 5.7. There is no justification for these restrictions.

Defendants assert that territorial limits are needed to "ensure compliance with applicable United States Export Administration Regulations." *See* Ex. B § 5.7. Plaintiffs have repeatedly asked Defendants to specify the "applicable" regulatory provision (or any other law) that would be violated if individuals reviewed Protected Material outside the United States (or if foreign nationals reviewed it within the United States). Defendants acknowledged in meet-and-confers that they have identified no such law. Plaintiff has likewise been unable to identify any such law. In reality, protective orders (including this District's Model Order) routinely authorize parties to access materials outside the United States, and this is because there is no legal prohibition on doing so.

Defendants also contend that individuals outside the United States may not be subject to personal jurisdiction for purposes of enforcing the Protective Order. This is not correct. Consultants (and others) cannot review Protected Material without first executing an

[1] Ignoring *Figaro*, Defendants point to a few *stipulated* protective orders supposedly containing the data security provisions they propose (*see supra* n.6). None of those orders involved security provisions as onerous or elaborate as what is proposed here, and in none of these cases were the provisions contested or evaluated in a judicial opinion.

"Acknowledgment and Agreement to be Bound," pursuant to which they must explicitly "agree to submit to the jurisdiction of the United States District Court for the Western District of Washington for the purpose of enforcing the terms of this Stipulated Protective Order." *See* Ex. A (Exhibit A thereto). Even without this provision, the Court can enforce the Protective Order through the Parties themselves, which are of course subject to this Court's jurisdiction.

In addition to being unjustified, Defendants' proposed territorial restrictions are ambiguous and thus unworkable in practice. If a document is hosted on a U.S. server, but accessed from a residence in Toronto, is that impermissible access from a foreign jurisdiction? What if a document vendor has a technician in London. Can that technician provide maintenance on the database? Defendants' ESI Protocols do not answer these (or the many) questions likely to arise in day-to-day litigation.

Last, Defendants' proposal is prejudicial because Plaintiff is consulting a number of non-U.S. economists in connection with this matter. If these consultants are unable to review Protected Material, as Defendants propose, they will not be able to provide meaningful assistance as this case progresses. This prejudice is readily averted by adhering to the District's Model Stipulated Protective Order, which contains robust and enforceable protections against unauthorized disclosures, without any arbitrary restrictions on the territories where Protected Material may be reviewed, or the nationalities of persons reviewing it.

Defendants' Statement

The parties have agreed on many provisions for the proposed Protective Order, but Plaintiff refuses to engage with Defendants on the implementation of critical data security and data export provisions. Although Plaintiff recognizes that data breaches are an actual threat, Plaintiff refuses to implement data security and data export requirements in the proposed Protective Order but does not articulate any inability to implement such provisions or how such requirements would prejudice Plaintiff. Defendants respectfully ask this Court to enter its proposed Protective Order (Ex. B), which includes reasonable provisions covering (1) data-security protections for electronic discovery and (2) export restrictions on discovery material.

Data Security. Organized criminal groups and hostile state actors are perpetrating data security attacks with growing frequency, and law firms and their vendors have increasingly become targets. The American Bar Association itself announced that it was the victim of a data breach in March 2023.[2] In 2022 alone, more than 100 law firms reported data breaches to authorities across 17 states, exceeding the 88 breaches and 46 breaches reported in 2021 and 2020, respectively.[3]

Recognizing these mounting concerns, the state of Washington in 2020 revised its data breach law to be even more stringent.[4] The Washington State Office of the Attorney General noted in a 2019 report that "[d]ata breaches continue to be a significant concern," and as breaches continue to occur it only "highlight[s] the importance of the data breach legislation passed in [Washington], which will require earlier and more detailed notice to [affected parties] of a breach for a greater variety of their data, giving Washington one of the most robust data breach laws in the nation."

In light of this real and mounting threat, protective orders should include adequate measures for handling electronic documents and data and responding to an actual or suspected data breach.[5] Multiple federal district courts in the Ninth Circuit have already approved

---

[2] Sara Merken, *ABA Says Hackers Took Lawyers' Data in March Attack*, Reuters (April 21, 2023), https://tinyurl.com/59pvfpz8.

[3] Xiumei Dong, *Law Firm Data Breaches Continue to Rise*, Law360 (Feb. 6, 2023), https://www.law360.com/pulse/articles/1573082/law-firm-data-breaches-continue-to-rise; *see also* Dan Roe, *Cyberattacks 'Inevitable' for Law Firms, Highlighting Need for Comprehensive Incident Response Plans*, The American Lawyer (Jan. 10, 2023), https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/?slreturn=20230401100619.

[4] HB 1071, Protecting Personal Information (2019), https://app.leg.wa.gov/billsummary?BillNumber=1071&Year=2019.

[5] Robert Hilson, *Why the archaic process of eDiscovery is vulnerable to hacking and data breach*, Logikcull (Feb. 8, 2017), tinyurl.com/mprnbvpz; *Data Breach Investigations Report*, Verizon (2022), verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf.

protective orders including such provisions.[6] The data security provisions Defendants now request follow suit and further align with steps that the State has already undertaken.[7]

Specifically, Defendants propose that the parties and their vendors implement security measures complying with at least one recognized cybersecurity framework, such as the Critical Security Controls published by the Center for Internet Security (CIS). Ex. B, § 9(1). These are industry-standard frameworks with which many vendors and law firms already comply. Accordingly, any burden imposed by this provision is minimal, and Plaintiff's assertion that the proposal is "not workable in practice" ignores that Defendants propose to require industry standard practices already in use. To mitigate the risk of unauthorized access, Defendants also propose that the parties encrypt protected materials in transit[8] (and at rest where reasonably practical) and implement multi-factor authentication (MFA) for access. Again, both of these security measures are regularly used in practice. MFA is a simple measure that has been called "the single most important thing Americans can do to stay safe online."[9] *Id.* § 9(1). A Party could satisfy this MFA requirement by registering users' computers as trusted devices, after which they can access protected materials with a password—a process commonly used across corporate America today.[10] Using passwords without more leaves materials vulnerable to attack, but MFA is a low-burden, highly effective security mechanism that Americans use every day

[6] *See*, *e.g.*, *Apple Inc., v. Rivos, Inc.*, Case No. 5:22-cv-2637, (N.D. Cal. Oct. 31, 2022) (Dkt. 113, § 8); *Sheet Metal Workers' Nat'l Pension Fund v. Bayer Aktiengesellschaft*, Case No. 3:20-cv-04737-RS (N.D. Cal. Oct. 6, 2022) (Dkt. 138, § 7.6); *Anderson v. Gen. Motors, LLC*, Case No.: 2:22-cv-00353-KJM-DMC (E.D. Cal. Sept. 6, 2022) (Dkt. 38, § 29); *K-fee Sys. GmbH v. Nespresso USA, Inc.*, 2:21-cv-3402-GW (C.D. Cal. Apr. 28, 2022) (Dkt. 159, § 32); *Teradata Corp. v. SAP SE*, Case No. 3:18-cv-03670-WHO (N.D. Cal. May 14, 2019) (Dkt. 98, § 15).

[7] *2019 Data Breach Report,* Washington State Attorney General's Office, at 26, https://agportal-s3bucket.s3.amazonaws.com/uploadedfiles/Another/News/Press_Releases/2019DBReport.pdf; *see also 2022 Data Breach Report,* Washington State Attorney General's Office, https://agportal-s3bucket.s3.amazonaws.com/DBR2022%20v5.pdf.

[8] *See Data Protection: Data In transit vs. Data At Rest*, DataInsider (Digital Guardian's Blog) (Nov. 28, 2022), tinyurl.com/t9kjat27.

[9] Jen Easterly, *Next Level MFA: FIDO Authentication*, Cybersecurity & Infrastructure Security Agency (Oct. 18, 2022), tinyurl.com/bdenbcxp; *see also* D. Howard Kass, *CISA Director Jen Easterly Issues Call to Action for Multi-factor Authentication, Passwordless Security*, MSSP Alert (Oct. 20, 2022), tinyurl.com/4hd4thyh; *see also*, *e.g.*, 16 C.F.R. § 314.4.

[10] *See*, *e.g.*, Eric Griffith, *Multi-Factor Authentication: Who Has It and How to Set It Up*, PCMag (Jan. 19, 2022), tinyurl.com/ez86rmt2.

(more often than they even realize).[11] Indeed, the federal judiciary requested funding to implement enterprise-wide MFA this fiscal year.[12] Yet, Plaintiff refuses to implement such security measures.

To facilitate prompt mitigation and remediation in the event of an actual or suspected data breach, Defendants also propose data breach provisions. Specifically, Defendants propose that the Party[13] incurring an actual breach notify the other Party within 48 hours.[14] *Id.* § 9(2). Defendants' proposal also provides for the Parties' cooperation following a breach to help effectively and expeditiously terminate and prevent unauthorized access. *Id.* §§ 9(3) - 9(4). Defendants propose that the Party incurring an actual breach submit to reasonable discovery concerning the breach as described in the proposed order, permitting the Parties to understand the related circumstances.[15] These provisions set clear expectations on basic steps for investigation after a breach. None of these provisions imposes significant burden, but taken together, they provide strong protections from real and serious dangers. Defendants go to great lengths to protect their customers' personal data, their partners' business information shared in confidence, and Defendants' own trade secrets and other sensitive information in the ordinary course of their business. *See*, *e.g.*, *Epic Games, Inc. v. Apple Inc.*, 559 F. Supp. 3d 898, 949 (N.D. Cal. 2021). Discovery in this case could involve sensitive consumer, financial, transactional, and business strategy data and information. In the event of any required disclosure, those materials should be safeguarded with *at least* minimum data security standards, as Defendants propose. Plaintiff's refusal to stipulate to these reasonable minimum standards is

---

[11] *See Multifactor Authentication*, Cybersecurity & Infrastructure Security Agency, cisa.gov/mfa ("Malicious cyber actors are increasingly capable of phishing or harvesting passwords to gain unauthorized access."); *What is: Multifactor Authentication*, Microsoft Support, tinyurl.com/385mkaat ("Almost every online service from your bank, to your personal email, to your social media accounts supports adding a second step of authentication").

[12] *See The Judiciary Fiscal Year 2023 Congressional Budget Request: Judiciary Information Technology Fund*, The Administrative Office of the U.S. Courts (Mar. 2022), tinyurl.com/32ruwm6w.

[13] Party is defined in the proposed Protective Order as, "[a]ny Party to this action, including all its officers, directors, employees, consultants, vendors, retained Experts, and Outside Counsel of Record (and their support staff)."

[14] *See also CIS Critical Security Control 17: Incident Response and Management*, CIS, tinyurl.com/ycy8a3bv ("Establish a program to develop and maintain an incident response capability . . . to prepare, detect, and quickly respond to an attack.").

[15] *Sedona Conference International Principles: Discovery, Disclosure & Data Protection In Civil Litigation*, Sedona Conference, at vi, 54 (Transitional ed. Jan. 2017), tinyurl.com/y25ehr67.

without merit. Additionally, his reliance on *Figaro* is unpersuasive because, there, the court indicated it was "concerned" about entering a different protective order than the "protective order in the [parallel] consumer action" which would "be entirely unclear what protective order applies to what." *See* Plaintiff's Ex. E at 5:8-11. Here, there would be no confusion as this case is the only action at issue. Finally, Plaintiff raises concerns about violations to the data security provision of the proposed Protective Order when filing documents with the Court. This is not the intention of the provision and Plaintiff had not raised such concerns until now. Defendants would be amenable to proposed language addressing these concerns.

All Parties would be subject to the same requirements, so any argument that these protocols unfairly burden one side is without merit. Defendants do not seek to implement unilateral obligations or to gain any litigation advantage. The proposed provisions are mutually applicable, reasonable, and appropriate to manage the risk to data produced by all Parties. There is no question that measures to prevent and remedy a breach of confidential materials constitute protection from expense, burden, annoyance, and embarrassment, *i.e.*, the purpose of a protective order under Rule 26(c)(1). The financial costs of a data breach alone justify requiring reasonable security measures of parties handling protected materials.[16] In light of ever-present and growing data-security threats, detailed data-security provisions are necessary. Plaintiff does not dispute that it is reasonable for a receiving Party to notify and reasonably cooperate with a producing Party whose protected materials are compromised in a data breach. Plaintiff simply does not want to be *required* to take these reasonable steps and, therefore, the Parties have been unable to reach agreement as to the appropriate data-security requirements.

Secure Storage, No Export. Similar to the data security provisions, Defendants believe that export restrictions on materials designated as Confidential or Highly Confidential in this litigation are reasonable and supported. The provision merely requires a Party to maintain protected material in a secure manner, as established in the Protective Order, at a location within the United States. This additional provision is important to protect Confidential and Highly

[16] *See Cost of a Data Breach Report 2022*, IBM Security at 5, tinyurl.com/2s3nmj65 ("Reaching an all-time high, the cost of a data breach averaged USD 4.35 million in 2022.").

Confidential Material because a protective order does not (and cannot) grant any federal court jurisdiction to enforce the protective order over people located in foreign countries necessary. *See Sound N Light Animatronics Co. v. Cloud B, Inc.,* 2017 WL 3081685, at *10 (C.D. Cal. Apr. 7, 2017). Plaintiff's suggestion that this issue is cured simply by signing the "Agreement to be Bound" misses the point, as the Court would still face difficulties in enforcing its order abroad. *See, e.g., Westerngeco LLC v. Ion Geophysical Corp*., 776 F. Supp. 2d 342, 367 n.17 (S.D. Tex. Mar. 2, 2011) ("Although a state may, in limited circumstances, extend its jurisdiction beyond the territorial limits of its sovereignty, any such extension is 'subject to the consent of other nations.'"). Additionally, depending on the scope of Plaintiff's discovery requests, discovery may encompass information subject to export control regulations, and such a provision would ensure compliance with these export security provisions, including Export Control Classification Numbers 5D002, 5E002, 5D992, 5E992, and EAR99, which restrict export out of the United States and disclosure to foreign persons and corporations.

Plaintiff provides no explanation for why such restriction should not be implemented and additionally, Plaintiff's attorneys have previously agreed to include such provisions in other lawsuits including *Anderson v. Apple* (Case No. 3:20-cv-02328-WHO (N.D. Cal.)), the fact that Plaintiff has previously agreed to such language in other matters renders argument that this provision is "ambiguous and [] unworkable" unpersuasive. Defendants believe these additional security requirements are justified and have been included in Ex. B, §§ 5.7, 5.2(b), and 5.4(b).

2. ESI Protocols

The Parties' only outstanding dispute on ESI Protocols concerns the provisions regarding ESI preservation obligations, as set forth below. The Parties' proposals on this issue, in addition to being described below, are set forth in their proposed ESI Protocols attached hereto as Exhibit C (Plaintiff's) and Exhibit D (Defendants'), respectively.

Plaintiff's Statement:

Plaintiffs propose that the Parties' obligation to preserve relevant ESI be governed by this Court's Model Agreement Regarding Discovery of Electronically Stored Information. The Model sets forth a definitive list of ESI categories that need not be preserved (*e.g.*, "Deleted, slack, fragmented, or other data only accessible by forensics."). *See* Ex. C § D.3. Plaintiffs propose adopting that list, but not inflexibly. Plaintiffs' ESI Protocols would also allow Parties to not preserve (*i.e.*, destroy) other categories of ESI, provided they confer and obtain agreement in advance. *See id.* § D.4.

Defendants counter with an unworkable departure from the Model Order. Under Defendants' ESI Protocols, the list of relevant ESI that need not be preserved is illustrative rather than definitive. Parties would be free to destroy other relevant ESI so long as they make a unilateral determination that its "duplicative" of other ESI being preserved. *See* Ex. D § D.3. But what counts as "duplicative" is not clear, nor can it be policed. Allowing Parties to unilaterally destroy relevant ESI based on their subjective determination that the ESI duplicates other ESI is a recipe for human error and abuse. The better approach, Plaintiff respectfully submits, is to follow the Model Order and require Parties to preserve *all* relevant ESI, subject to clearly defined carveouts.

Defendants raise concerns as to the burden of preserving relevant ESI in all available forms, but this can be accommodated through the meet-and-confer process Plaintiff has proposed. That is, if Defendants identify a particular category of ESI that is "duplicative" and burdensome to preserve, Defendants can raise the issue and the Parties will work to resolve it in good faith. This is exactly what this District's Model Order contemplates. *See* Model ESI Order § D.3 ("The parties should confer regarding any other categories of ESI that may not need to be preserved."). Below, Defendants characterize this as an "entirely unworkable" and "impractical directive," forgetting that the Model Order reflects the accrued experience of this District in managing ESI discovery.

Defendants' Statement:

As the Federal Rules and the agreed-upon provisions of the ESI Protocol require, Defendants have been and will continue to preserve discoverable information pertinent to this litigation. Their efforts to fulfill their preservation duties include appropriate litigation holds to preserve relevant ESI from relevant custodians and data sources. Both Defendants have robust litigation support mechanisms, and Plaintiff does not and cannot suggest that they are incapable of appropriate retention of ESI while litigation is pending.

Even so, Plaintiff seeks to include additional provisions regarding the storage of non-relevant data sources, which are impractical, unnecessary, and impose heavy burdens disproportionate to any legitimate need. *See* Ex. C at D.5.

First, Plaintiff refuses to agree that *duplicative, non-unique* documents need not be preserved—even when Defendants have explained that they will preserve (and treat as unique) copies of same document held by more than one custodian. Plaintiff does not show why preservation of true duplicates of a single custodian is relevant or proportionate to the needs of his case. To the contrary, courts regularly hold that applying preexisting preservation policies to duplicate ESI is harmless and reasonable. *See, e.g.*, *United States v. Stewart*, 420 F.3d 1007, 1021 & n.13 (9th Cir. 2005) (permitting copy digital recording as evidence where government did not preserve the duplicated original, absent indication of alteration); *FTC v. Lights of Am. Inc.*, 2012 WL 695008, at *5 (C.D. Cal. Jan. 20, 2012) ("auto-delete policy [deleting duplicates] is consistent with [a party's] duty to preserve relevant material" where copies were preserved through litigation hold). "[N]eedless retention of documents… slows the system" and unduly burdens Defendants with costly data storage, without any benefit to Plaintiff for whom the *exact same* information will be available in duplicate form. *Lights of Am.*, 2012 WL 695008, at *5. Indeed, under *both* sides' proposed ESI protocols, productions may be de-duplicated, even across custodians, *see* Ex. A and B at C.4. Plaintiff shows no good cause to require Defendants to incur the burdens of preserving true duplicate ESI within a single custodian's file, particularly since he agrees he will never receive those duplicate copies. The Court should adopt Defendants'

proposed provision to specify in the ESI protocol that duplicate ESI need not be preserved.

Second, Plaintiff proposes to add a new provision to require the Parties to provide notice and confer before the deletion of categories of ESI not expressly included in the list of ESI that need not be preserved, and he opposes Defendants' language clarifying that the list is not exhaustive. Plaintiff's draft warps the Model ESI Agreements statement that the parties should confer regarding additional categories of ESI that need not be preserved into a highly burdensome and impractical directive that any Party intending not to preserve ESI of any kind, whether relevant or not, alert the other Parties in advance and confer about doing so.

This proposal is entirely unworkable. Plaintiff's proposed addition would require Amazon and Apple to apprise him about all manner of routine data and document deletion, regardless of its potential relevance to this litigation. The addition does not limit the obligation it creates to information pertinent to this case, even though the Federal Rules cabin the duty to preserve to what would be discoverable. And even if Plaintiff's proposal did contain such a limitation, all that does is add risk to a Party's routine deletion of data and documents not anticipated to be discoverable (and thus excluded from a litigation hold), should the other side choose to see it differently. It does not remove the chance of "human error" as Plaintiff contends; it only makes that possibility higher stakes in a way not contemplated by the Federal Rules' emphasis on reasonability. Nor does Plaintiff have any basis to suggest "abuse" by Defendants, who are well aware of their document-preservation obligations.

These issues disproportionately burden Defendants, both of whom are large companies with hundreds of thousands (or more) employees and significant quantities of documents and data having nothing to do with this litigation. As Plaintiff's current proposal reads there is no limitation on the ESI that is subject to this provision, including potentially ESI that is maintained by Defendants' employees not identified as relevant custodians in this litigation. The current provision as written would also apply to employees located outside of the United States and may conflict with other obligations not to maintain certain types of data in those jurisdictions.

As explained above, both Defendants take their preservation obligations seriously and

have implemented appropriate and reasonable controls to ensure that relevant ESI is preserved for this litigation. Requiring them to consult with Plaintiff's counsel about—and *before*—deleting or otherwise declining to preserve ESI not subject to those controls would be costly, time intensive, and heavily burdensome on Defendants' businesses. And doing so is unlikely to garner for Plaintiff any additional discoverable information, while risking pointless squabbles about what may or may not turn out to be discoverable and distracting from the core issues in this case. The Court should reject Plaintiff's effort to expand Defendants' preservation obligations beyond what the Federal Rules contemplate, which would heavily burden Defendants. It should instead adopt Defendants' proposed ESI protocol, Ex. D, which tracks those obligations and ensures the preservation of ESI necessary for this case.

DATED this 3rd day of May, 2023

HAGENS BERMAN SOBOL SHAPIRO LLP

By /s/ *Steve W. Berman*
Steve W. Berman (WSBA No. 12536)

By /s/ *Barbara A. Mahoney*
Barbara A. Mahoney (WSBA No. 31845)
1301 Second Avenue Suite 2000
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com
barabaram@hbsslaw.com

Ben M. Harrington (*pro hac vice*)
Benjamin J. Siegel (*pro hac vice*)
715 Hearst Avenue, Suite 300
Berkeley, CA 94710
Telephone: (510) 725-3000
Facsimile: (510) 725-3001
benh@hbsslaw.com
bens@hbsslaw.com

Attorneys for Plaintiff and the Proposed Class

ORRICK, HERRINGTON & SUTCLIFFE LLP

By: /s/ *Mark S. Parris*
Mark S. Parris (WSBA No. 18370)
mparris@orrick.com
401 Union Street, Suite 3300
Seattle, WA 98101
Telephone: +1 206 839 4300
Facsimile: +1 206 839 4301

WEIL GOTSHAL & MANGES, LLP

By: */s/ Carrie C. Mahan*
Carrie C. Mahan (Pro Hac Vice)
carrie.mahan@weil.com

By: /s/ *S. Nicole Booth*
Sandra Nicole Booth (Pro Hac Vice)
nicole.booth@weil.com

2001 M. Street NW, Suite 600
Washington, DC 20036
Telephone: +1 202 682 7000

By: /s/ *Brian G. Liegel*
Brian G. Liegel (Pro Hac Vice)
brian.liegel@weil.com

1395 Brickell Avenue, Suite 1200
Miami, FL 33131
Telephone: +1 305 577 3180

Attorneys for APPLE INC.

By */s/ John Goldmark*

John Goldmark, WSBA #40980
MaryAnn Almeida, WSBA #49086
DAVIS WRIGHT TREMAINE, LLP
920 Fifth Avenue, Suite 3300
Seattle, Washington, 98104
Phone: (206) 622-3150
Fax: (206) 757-7700
Email: johngoldmark@dwt.com
maryannalmeida@dwt.com

Chad S. Hummel (*pro hac vice*)
SIDLEY AUSTIN LLP
1999 Avenue of the Stars, 17th Floor
Los Angeles, CA 90067
Phone: (310) 595-9500
Fax: (310) 595-9501
Email: chummel@sidley.com

Jonathan E. Nuechterlein (*pro hac vice*)
Benjamin M. Mundel (*pro hac vice*)
SIDLEY AUSTIN LLP
1501 K Street, N.W.
Washington, D.C. 20005
Phone: (202) 736-8000
Fax: (202) 736-8711
Email: jnuechterlein@sidley.com
bmundel@sidley.com

Attorneys for AMAZON.COM, INC.